Fig. 1

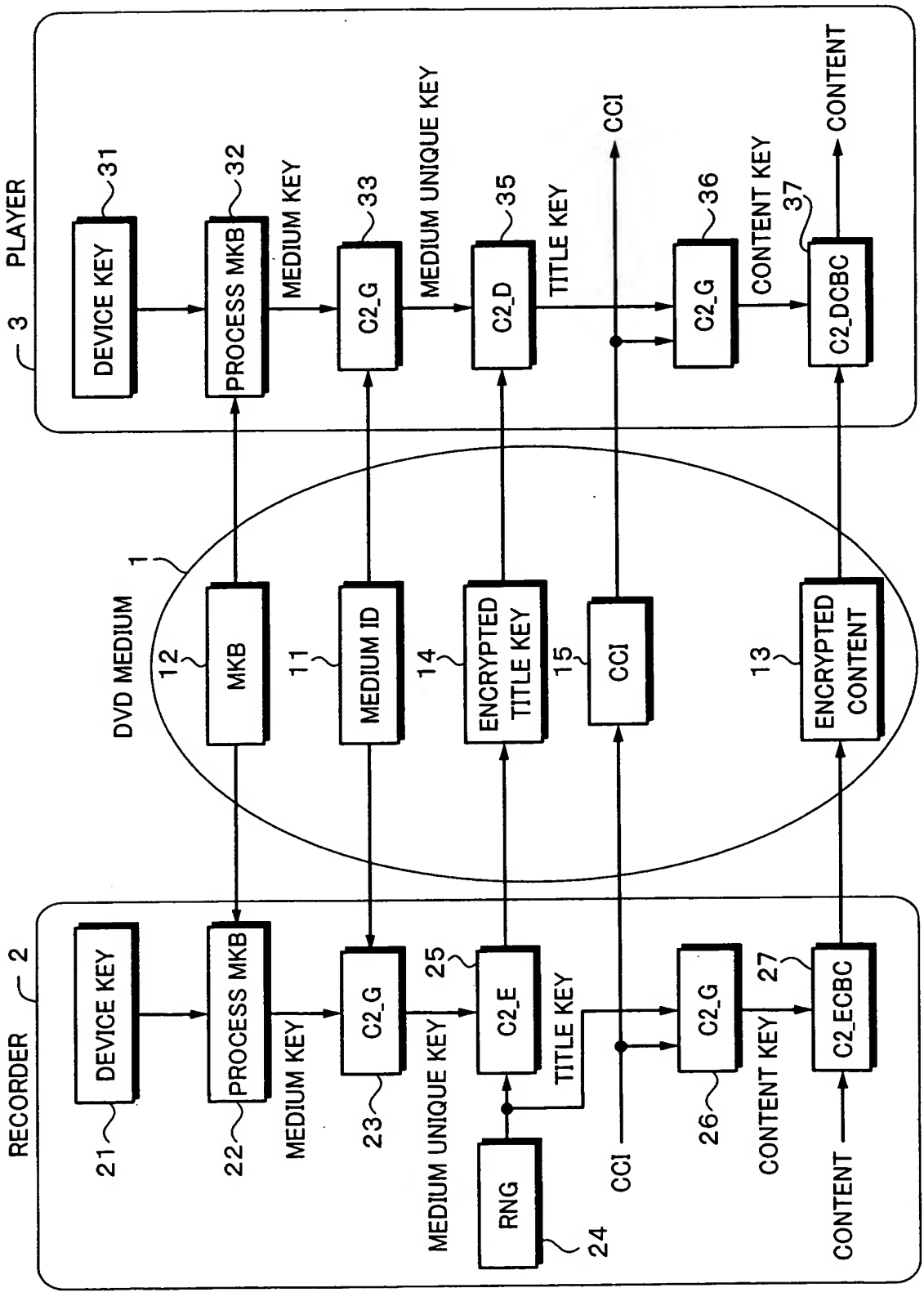

RECORDER
2
PLAYER
3
DVD MEDIUM
1
DEVICE KEY
21
PROCESS MKB
22
MEDIUM KEY
C2_G
23
MEDIUM UNIQUE KEY
25
C2_E
TITLE KEY
RNG
24
CCI
C2_G
26
CONTENT KEY
27
C2_ECBC
CONTENT
MKB
12
MEDIUM ID
11
ENCRYPTED TITLE KEY
14
15
CCI
ENCRYPTED CONTENT
13
DEVICE KEY
31
PROCESS MKB
32
MEDIUM KEY
C2_G
33
MEDIUM UNIQUE KEY
C2_D
35
TITLE KEY
CCI
C2_G
36
CONTENT KEY
37
C2_DCBC
CONTENT

Fig. 2

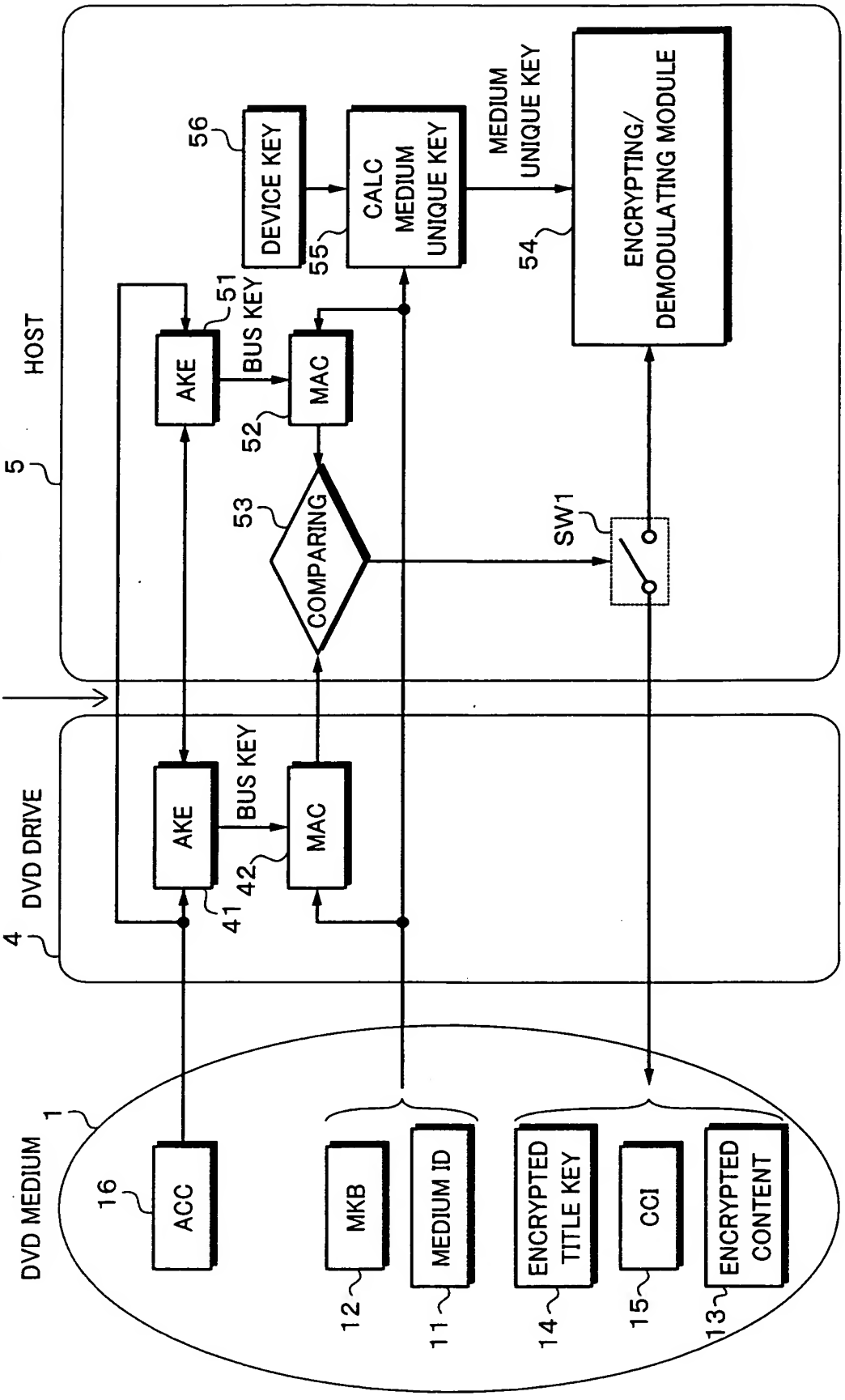

DVD MEDIUM
1
ACC
16
MKB
12
MEDIUM ID
11
ENCRYPTED TITLE KEY
14
CCI
15
ENCRYPTED CONTENT
13
4a DRIVE-HOST INTERFACE
4 DVD DRIVE
AKE
41
BUS KEY
MAC
42
5 HOST
AKE
51
BUS KEY
MAC
52
53
COMPARING
SW1
DEVICE KEY
56
CALC MEDIUM UNIQUE KEY
55
MEDIUM UNIQUE KEY
ENCRYPTING/ DEMODULATING MODULE
54

Fig. 3

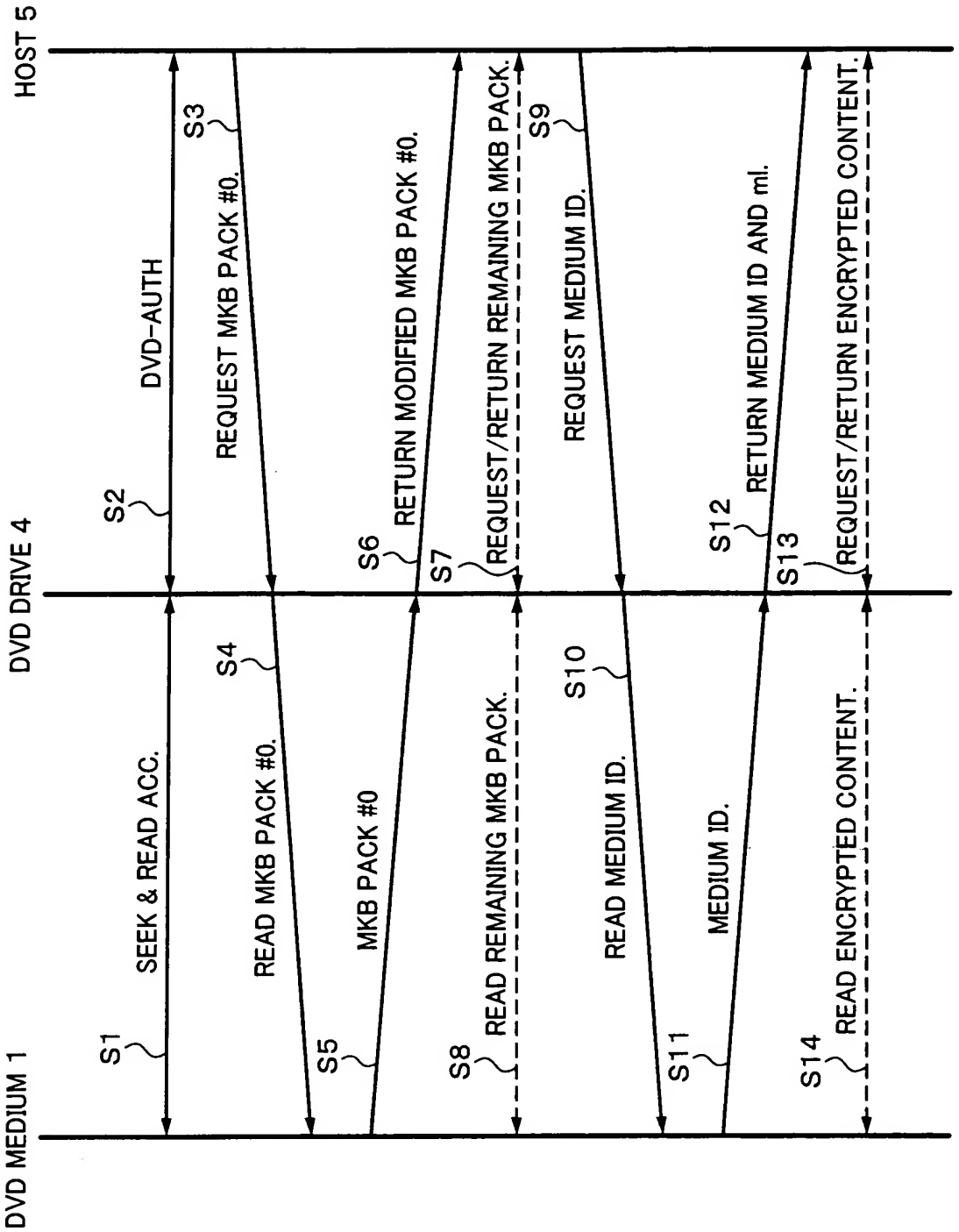

HOST 5
DVD DRIVE 4
DVD MEDIUM 1
S1
SEEK & READ ACC.
S2
DVD-AUTH
S3
REQUEST MKB PACK #0.
S4
READ MKB PACK #0.
S5
MKB PACK #0
S6
RETURN MODIFIED MKB PACK #0.
S7
REQUEST/RETURN REMAINING MKB PACK.
S8
READ REMAINING MKB PACK.
S9
REQUEST MEDIUM ID.
S10
READ MEDIUM ID.
S11
MEDIUM ID.
S12
RETURN MEDIUM ID AND ml.
S13
REQUEST/RETURN ENCRYPTED CONTENT.
S14
READ ENCRYPTED CONTENT.

Fig. 4

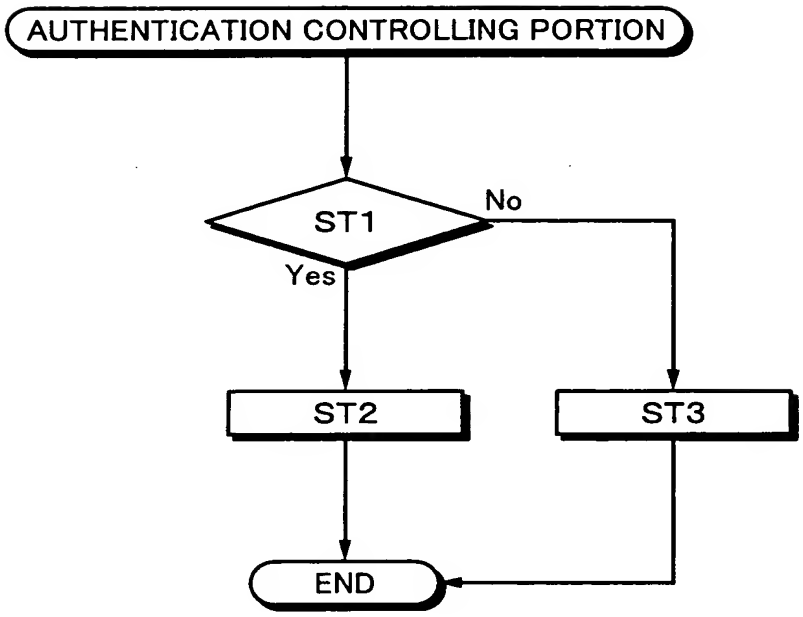


Fig. 5

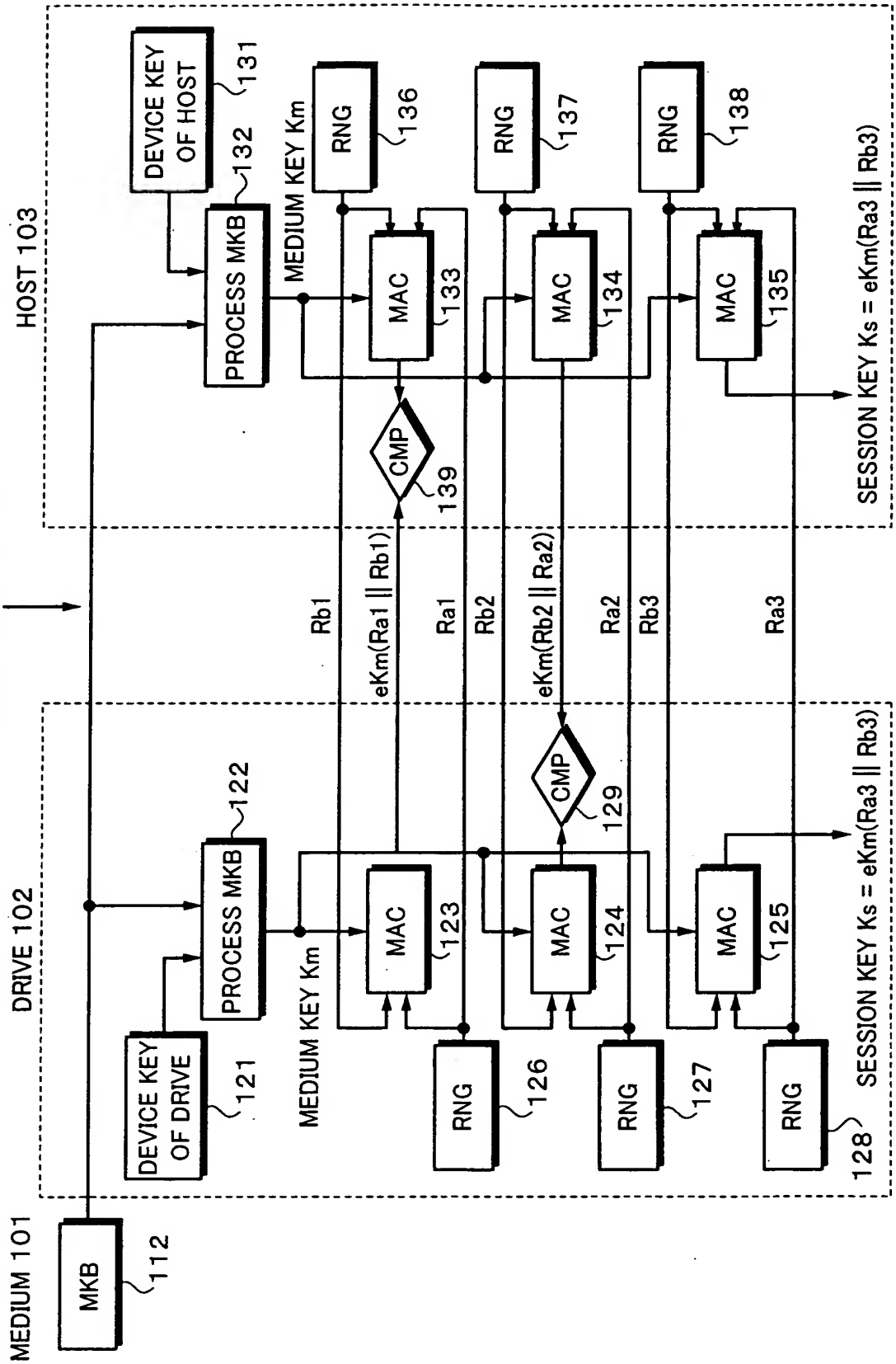

MEDIUM 101
MKB
112
DRIVE 102
DEVICE KEY OF DRIVE
121
PROCESS MKB
122
MEDIUM KEY Km
MAC
123
MAC
124
MAC
125
RNG
126
RNG
127
RNG
128
CMP
129
DRIVE-HOST I/F 104
Rb1
eKm(Ra1 || Rb1)
Ra1
Rb2
eKm(Rb2 || Ra2)
Ra2
Rb3
Ra3
SESSION KEY Ks = eKm(Ra3 || Rb3)
HOST 103
DEVICE KEY OF HOST
131
PROCESS MKB
132
MEDIUM KEY Km
MAC
133
MAC
134
MAC
135
RNG
136
RNG
137
RNG
138
CMP
139
SESSION KEY Ks = eKm(Ra3 || Rb3)

Fig. 6

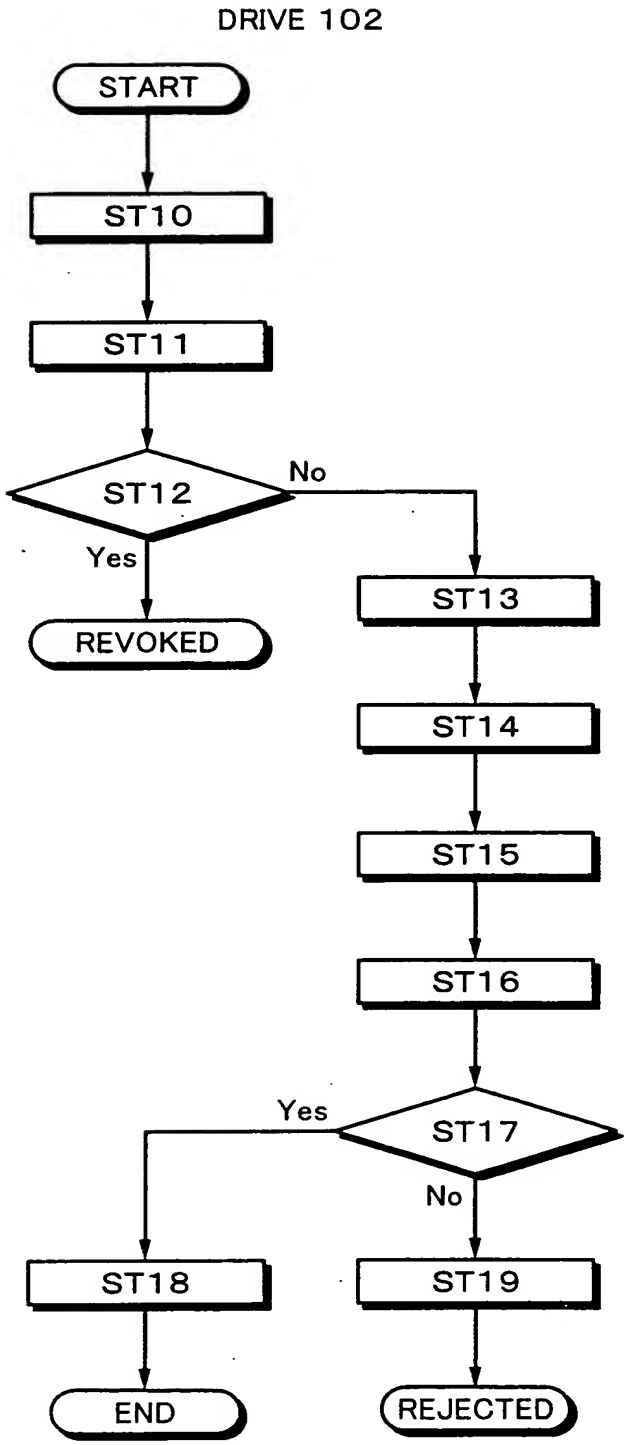

DRIVE 102
START
ST10
ST11
ST12
No
Yes
REVOKED
ST13
ST14
ST15
ST16
Yes
ST17
No
ST18
ST19
END
REJECTED

Fig. 7

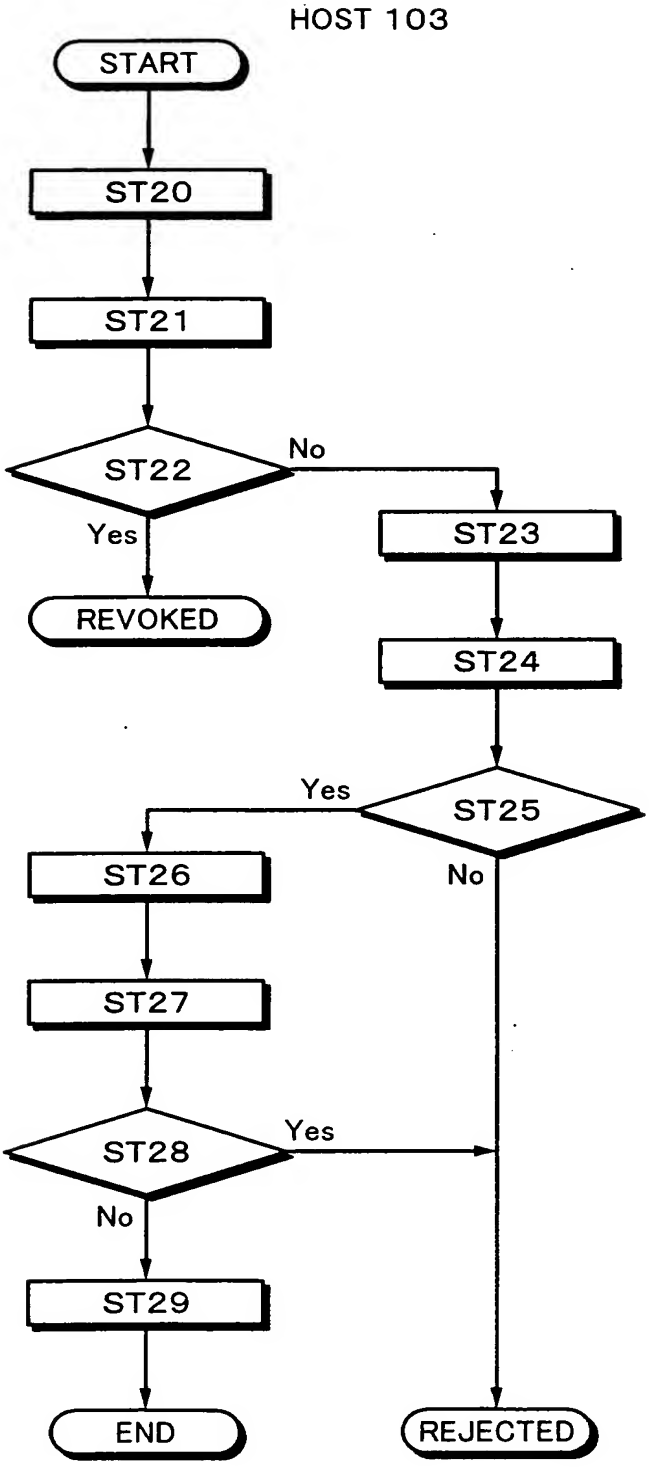

HOST 103
START
ST20
ST21
ST22
No
Yes
REVOKED
ST23
ST24
ST25
Yes
No
ST26
ST27
ST28
Yes
No
ST29
END
REJECTED

Fig. 8

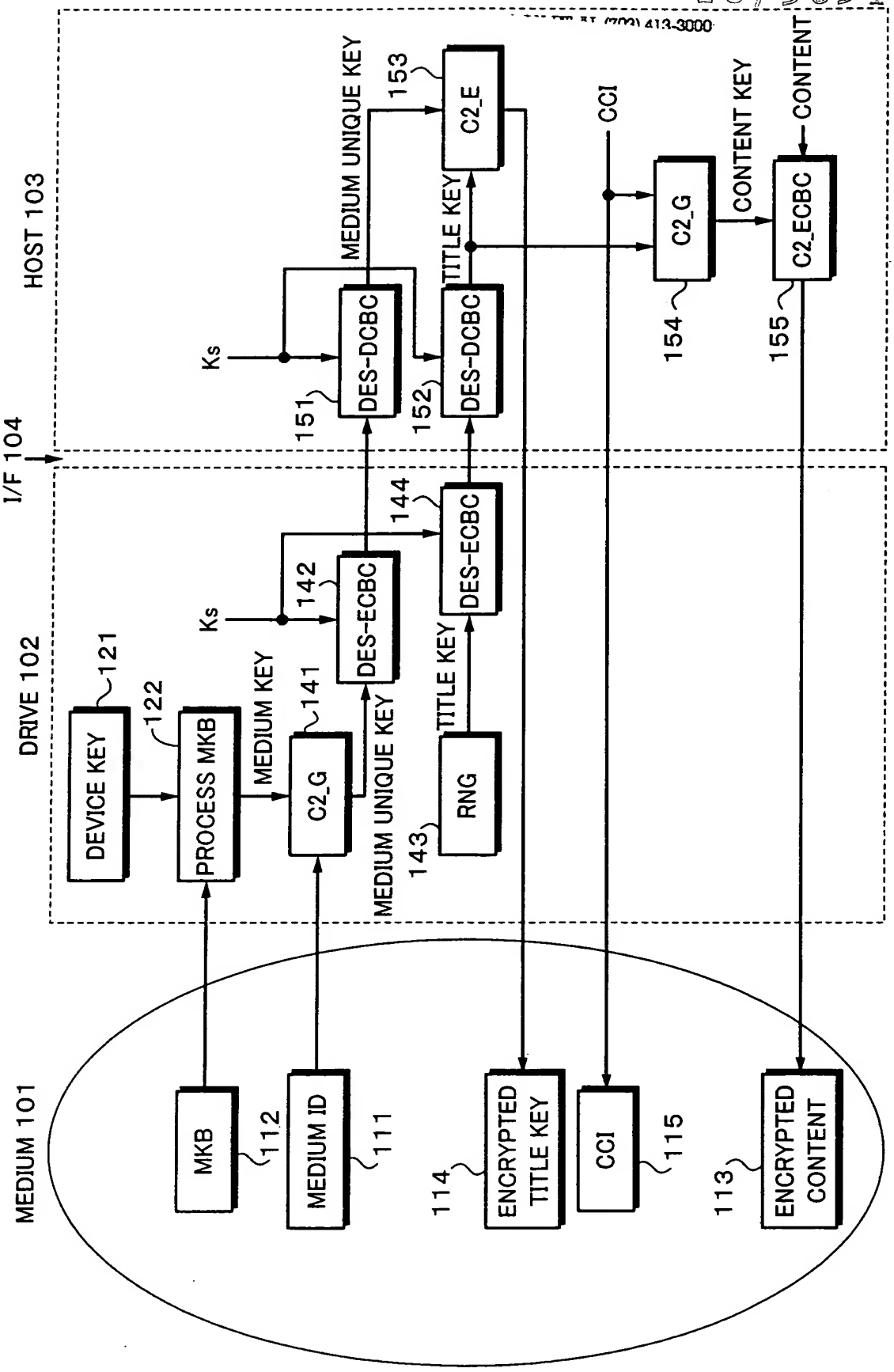

MEDIUM 101
HOST 103
I/F 104
DRIVE 102
MKB
112
MEDIUM ID
111
ENCRYPTED TITLE KEY
114
CCI
115
ENCRYPTED CONTENT
113
DEVICE KEY
121
PROCESS MKB
122
MEDIUM KEY
C2_G
141
Ks
142
DES-ECBC
MEDIUM UNIQUE KEY
RNG
143
TITLE KEY
144
DES-ECBC
DES-DCBC
151
DES-DCBC
152
MEDIUM UNIQUE KEY
153
C2_E
TITLE KEY
CCI
C2_G
154
CONTENT KEY
C2_ECBC
155
CONTENT

Fig. 9

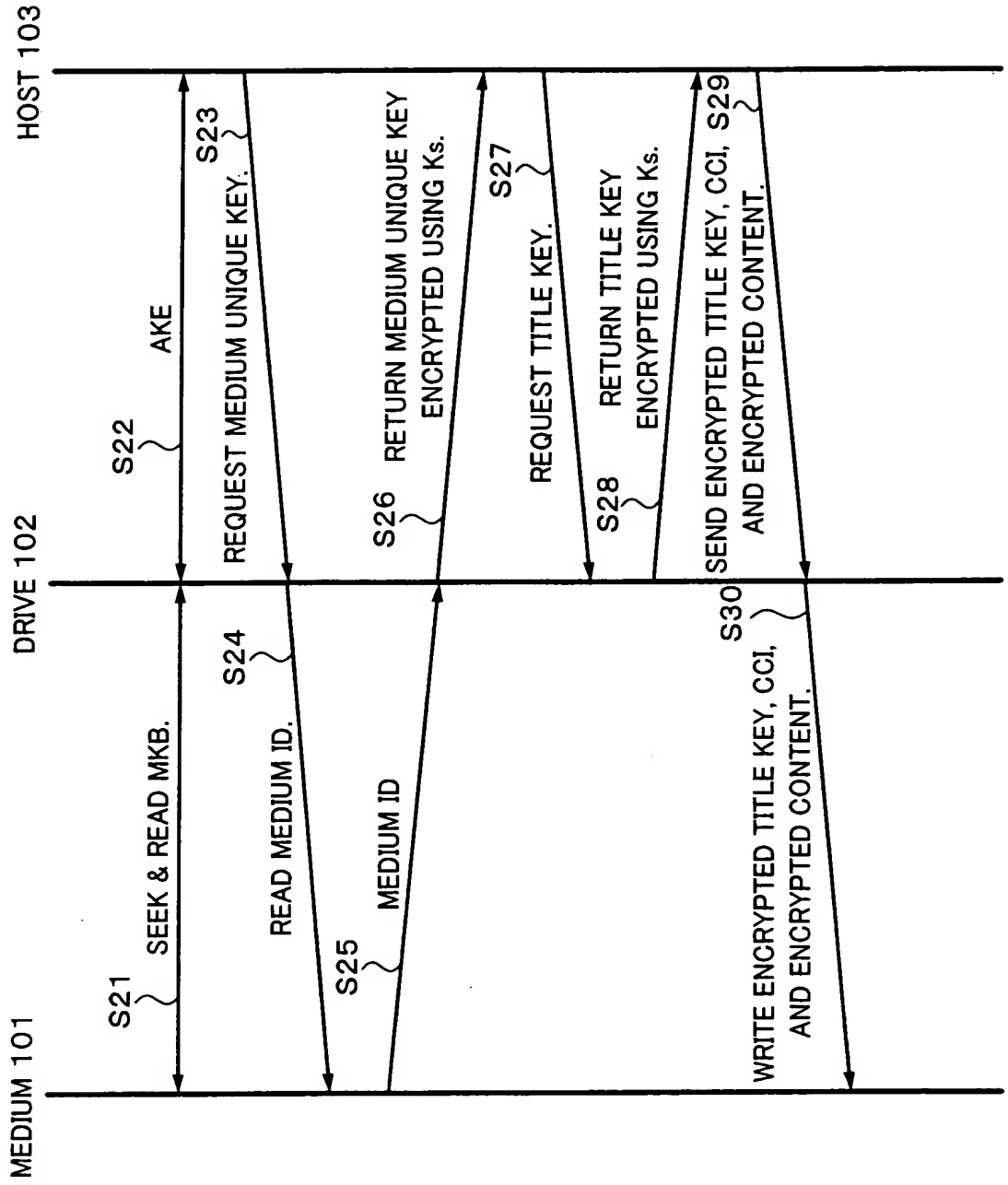

HOST 103
DRIVE 102
MEDIUM 101
S21
SEEK & READ MKB.
S22
AKE
S23
REQUEST MEDIUM UNIQUE KEY.
S24
READ MEDIUM ID.
S25
MEDIUM ID
S26
RETURN MEDIUM UNIQUE KEY ENCRYPTED USING Ks.
S27
REQUEST TITLE KEY.
S28
RETURN TITLE KEY ENCRYPTED USING Ks.
S29
SEND ENCRYPTED TITLE KEY, CCI, AND ENCRYPTED CONTENT.
S30
WRITE ENCRYPTED TITLE KEY, CCI, AND ENCRYPTED CONTENT.

Fig. 10

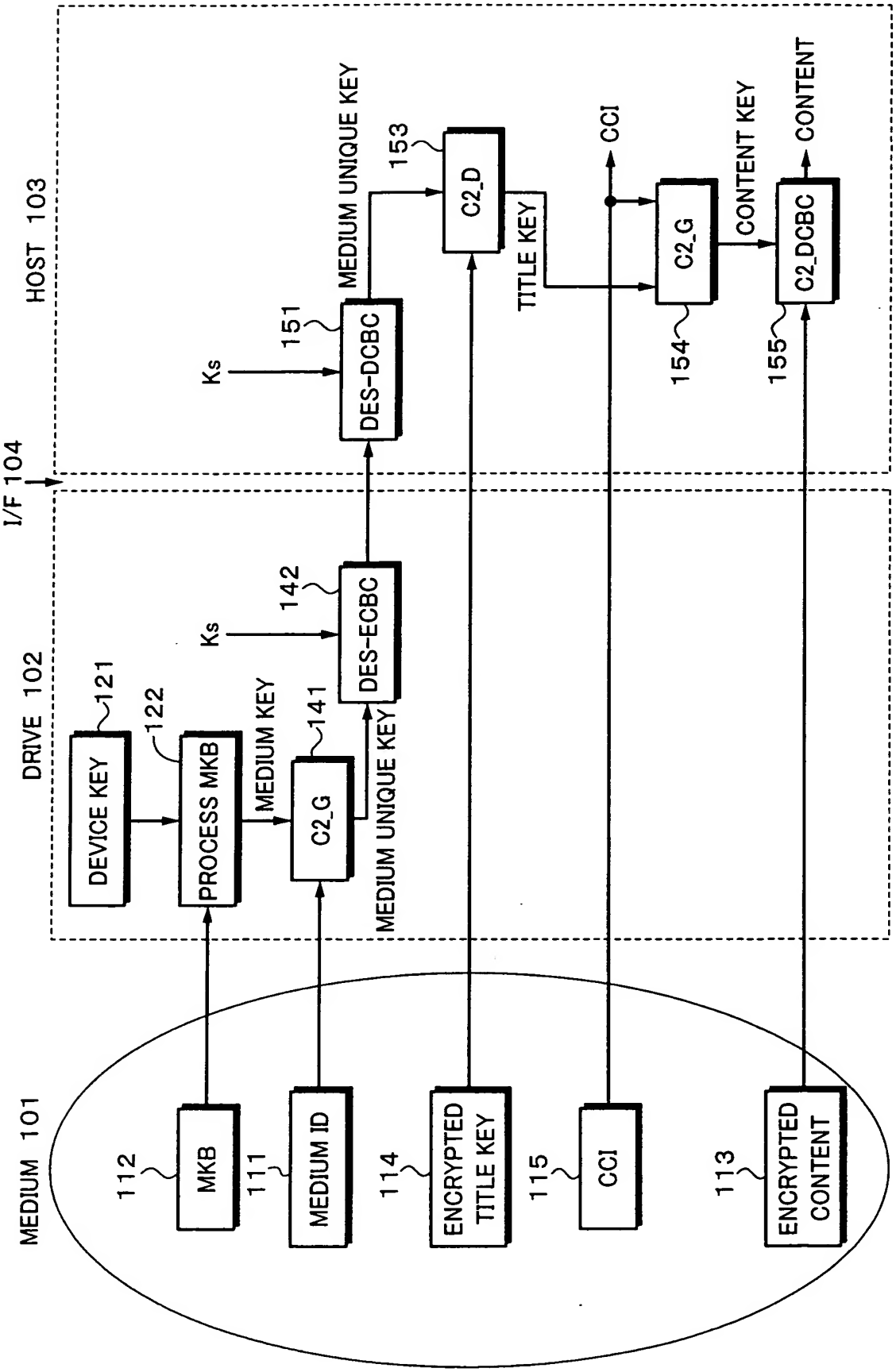

HOST 103
I/F 104
DRIVE 102
MEDIUM 101
MEDIUM UNIQUE KEY
153
C2_D
CCI
CONTENT KEY
CONTENT
Ks
151
DES-DCBC
TITLE KEY
C2_G
C2_DCBC
154
155
Ks
142
DES-ECBC
DEVICE KEY
121
PROCESS MKB
122
MEDIUM KEY
C2_G
141
MEDIUM UNIQUE KEY
MKB
112
MEDIUM ID
111
ENCRYPTED TITLE KEY
114
CCI
115
ENCRYPTED CONTENT
113

Fig. 11

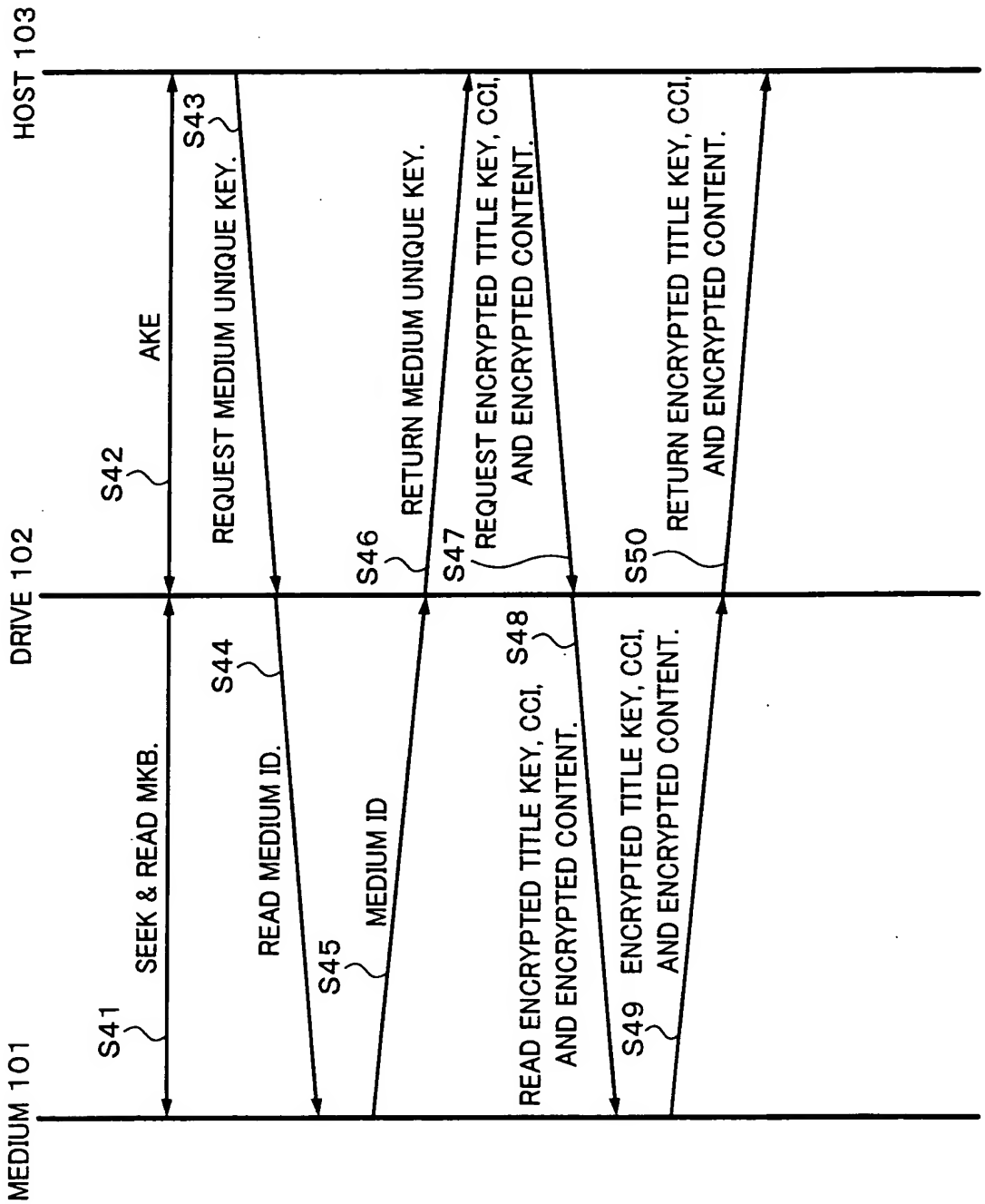

HOST 103
DRIVE 102
MEDIUM 101
S41
SEEK & READ MKB.
S42
AKE
S43
REQUEST MEDIUM UNIQUE KEY.
S44
READ MEDIUM ID.
S45
MEDIUM ID
S46
RETURN MEDIUM UNIQUE KEY.
S47
REQUEST ENCRYPTED TITLE KEY, CCI, AND ENCRYPTED CONTENT.
S48
READ ENCRYPTED TITLE KEY, CCI, AND ENCRYPTED CONTENT.
S49
ENCRYPTED TITLE KEY, CCI, AND ENCRYPTED CONTENT.
S50
RETURN ENCRYPTED TITLE KEY, CCI, AND ENCRYPTED CONTENT.

Fig. 12

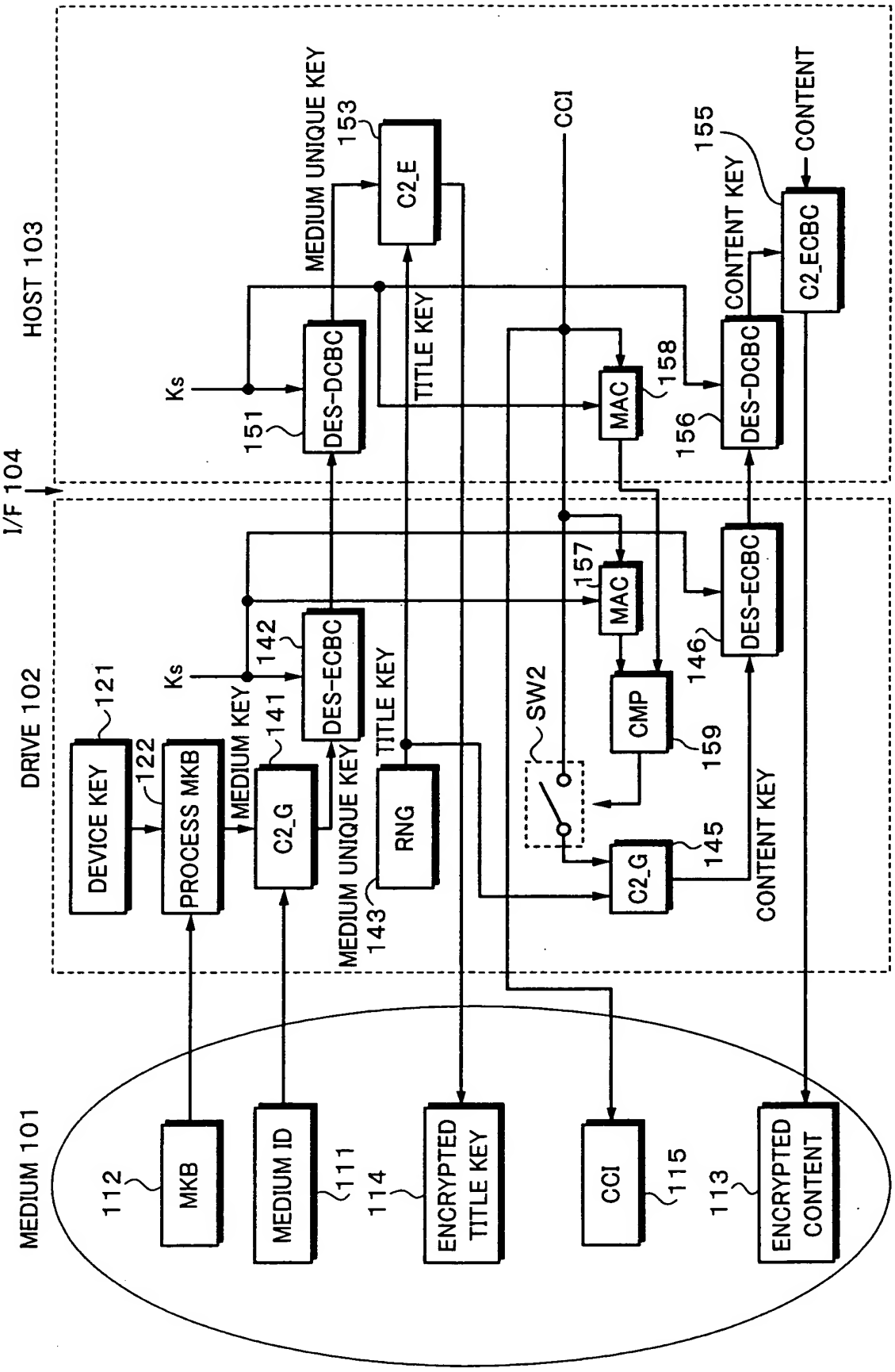
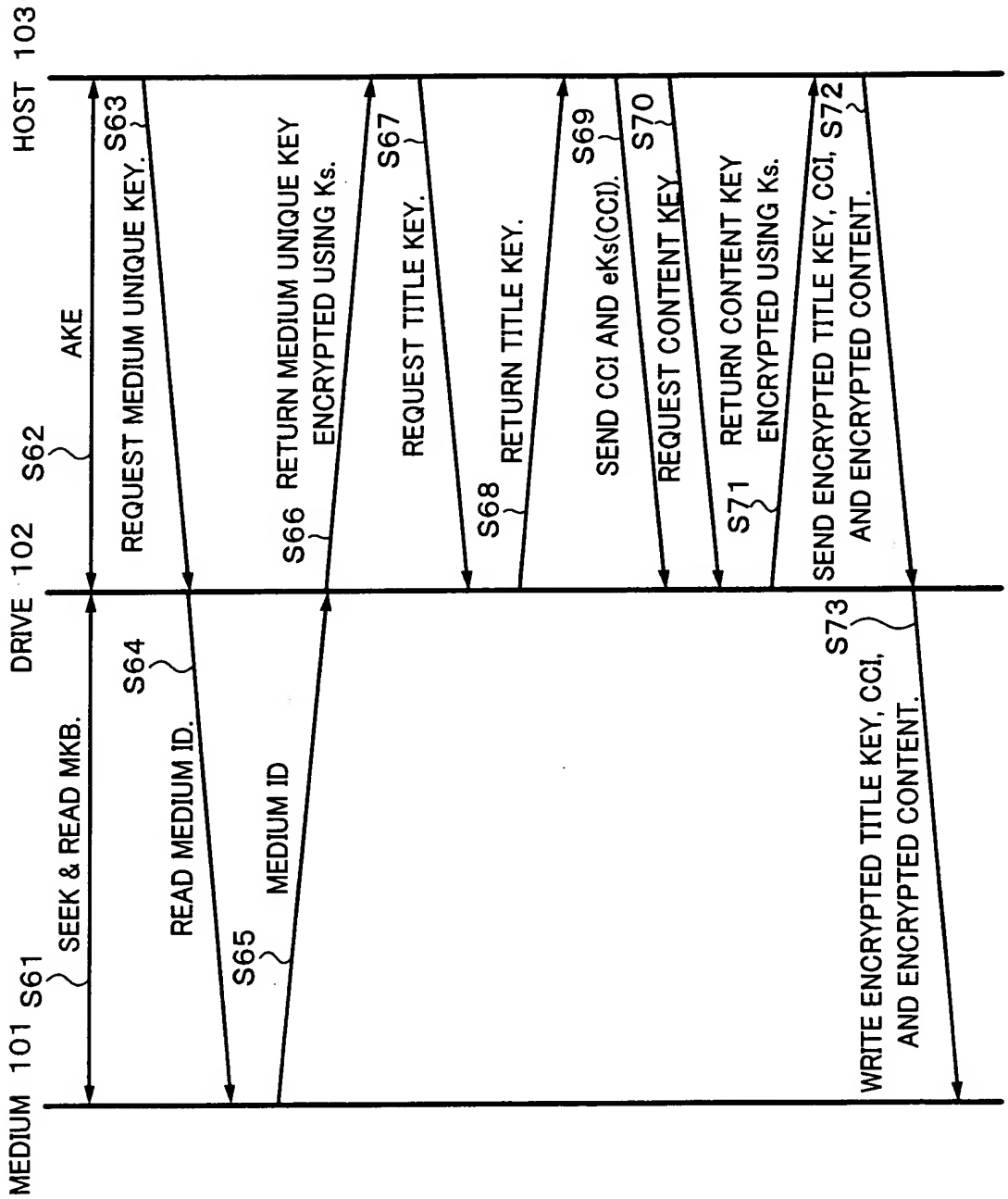

HOST 103
I/F 104
DRIVE 102
MEDIUM 101
MEDIUM UNIQUE KEY
153
C2_E
CCI
155
CONTENT KEY
CONTENT
C2_ECBC
Ks
151
DES-DCBC
TITLE KEY
MAC
158
156
DES-DCBC
157
MAC
DES-ECBC
146
SW2
CMP
159
DEVICE KEY
121
PROCESS MKB
122
MEDIUM KEY
141
C2_G
Ks
142
DES-ECBC
TITLE KEY
MEDIUM UNIQUE KEY
143
RNG
C2_G
145
CONTENT KEY
MKB
112
MEDIUM ID
111
ENCRYPTED TITLE KEY
114
CCI
115
ENCRYPTED CONTENT
113

Fig. 13


HOST 103
DRIVE 102
MEDIUM 101
S61
SEEK & READ MKB.
S62
AKE
S63
REQUEST MEDIUM UNIQUE KEY.
S64
READ MEDIUM ID.
S65
MEDIUM ID
S66
RETURN MEDIUM UNIQUE KEY ENCRYPTED USING Ks.
S67
REQUEST TITLE KEY.
S68
RETURN TITLE KEY.
S69
SEND CCI AND eKs(CCI).
S70
REQUEST CONTENT KEY
S71
RETURN CONTENT KEY ENCRYPTED USING Ks.
S72
SEND ENCRYPTED TITLE KEY, CCI, AND ENCRYPTED CONTENT.
S73
WRITE ENCRYPTED TITLE KEY, CCI, AND ENCRYPTED CONTENT.

DESCRIPTION OF REFERENCE NUMERALS

1	DVD MEDIUM
2	RECORDER
3	PLAYER
4	DVD DRIVE
4a	INTERFACE
5	HOST
11	MEDIUM ID
12	MEDIUM KEY BLOCK (MKB)
13	ENCRYPTED CONTENT
42, 52	MAC CALCULATING BLOCK
46	DEVICE KEY
46a	FIRST HALF PORTION OF DEVICE KEY
47	DES ENCRYPTOR
48	MEDIUM UNIQUE KEY CALCULATING BLOCK
49, 49a	DES ENCRYPTOR
49b	DES DECRYPTOR
53	COMPARING PORTION THAT COMPARE MACS
54	ENCRYPTING/DECRYPTING MODULE
55	MEDIUM UNIQUE KEY CALCULATING BLOCK
101	MEDIUM
102	DRIVE
103	HOST
104	INTERFACE
121	DEVICE KEY OF DRIVE

122	PROCESS MKB
123, 124, 125	MAC CALCULATING BLOCK OF DRIVE
126, 127, 128	RANDOM NUMBER GENERATOR OF DRIVE
129	COMPARING
131	DEVICE KEY OF HOST
132	PROCESS MKB
133, 134, 135	MAC CALCULATING BLOCK OF HOST
136, 137, 138	RANDOM NUMBER GENERATOR OF HOST
139	COMPARING
141, 154	C2_G
142, 144	DES ENCRYPTOR
143	RANDOM NUMBER GENERATOR
151, 152, 156	DES DECRYPTOR
153	C2_E
155	C2_EBC
157, 158	MAC CALCULATING BLOCK
159	COMPARING
ST1	MAC CALCULATED VALUES MATCH ?
ST2	TURN ON SWITCH.
ST3	TURN OFF SWITCH.
ST10	REPORT KEY (MKB)
ST11	CALCULATE MEDIUM KEY Km.
ST12	REVOKED ?
ST13	RECEIVE (Rb1, Rb2).
ST14	RETURN (eKm(Ra1 || Rb1), Ra1).

ST15 RETURN (Ra2, Ra3).

ST16 RECEIVE (eKm(Rb2 || Ra2), Rb3).

ST17 SAME MAC ?

ST18 SESSION KEY CONFIRMED (eKm(Ra3 || Rb3)

ST19 RETURN (ERROR)

ST20 REPORT KEY (MKB)

ST21 CALCULATE MEDIUM KEY Km.

ST22 REVOKED ?

ST23 SEND KEY (Rb1, Rb2).

ST24 REPORT KEY (eKm(Ra1 || Rb1), Ra1)

ST25 SAME MAC ?

ST26 REPORT KEY (Ra2, Ra3)

ST27 SEND KEY (eKm(Rb2 || Ra2), Rb3)

ST28 ERROR ?

ST29 SESSION KEY CONFIRMED (eKm(Ra3 || Rb3))